Frank S. Hedin (SBN 291289)
Hedin LLP
535 Mission Street, 14th Floor
San Francisco, CA 94105
Telephone: (305) 357-2107
Facsimile: (305) 200-8801
E-Mail: fhedin@hedinllp.com

Attorney for Plaintiff and the Putative Class

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

ALAN SILVA, individually and on behalf of all others similarly situated, Plaintiff, v. YANKA INDUSTRIES, INC. D/B/A MASTERCLASS, Defendant.	Case No. _____ **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff Alan Silva, individually and on behalf of all others similarly situated, makes the following allegations pursuant to the investigation of counsel and based upon information and belief, except as to allegations pertaining specifically to himself or his counsel, which are based on personal knowledge.

NATURE OF THE CASE

1. Plaintiff brings this action for legal and equitable remedies to redress and put a stop to Defendant Yanka Industries Inc. d/b/a MasterClass's practices of knowingly selling, transmitting, and/or otherwise disclosing, to various third parties, records containing the personal information (including names and addresses) of each of their subscribers, along with detailed information revealing the titles and subject

matter of the videos and other audiovisual materials purchased by each customer (collectively "Personal Viewing Information") in violation of the Video Privacy Protection Act, 18 U.S.C. §2701et. seq. ("VPPA").

2. Over the past two years, Defendant has systematically transmitted (and continues to transmit today) its subscribers' personally identifying video viewing information to Meta using a snippet of programming code called the "Meta Pixel," which Defendant chose to install on its masterclass.com website.

3. The information Defendant disclosed (and continues to disclose) to Meta, via the Meta Pixel it installed on its website, includes the subscriber's Facebook ID ("FID") coupled with the title of each of the specific videos that the subscriber requested on Defendant's website. A subscriber's FID is a unique sequence of numbers linked to the Meta profile belonging to that subscriber. The subscriber's Meta profile, in turn, publicly identifies the subscriber by name (and contains other personally identifying information about the subscriber as well). Entering "facebook.com/[FID]" into a web browser returns the Meta profile of the person to whom the FID corresponds. Thus, the FID identifies a person more precisely than a name, as numerous persons may share the same name but each person's Facebook profile (and associated FID) uniquely identifies one and only one person. In the simplest terms, the Meta Pixel installed by Defendant captures and discloses to Meta information that reveals the specific videos that a particular person viewed as a subscriber of Defendant's website (hereinafter, "Private Viewing Information").

4. Defendant disclosed and continues to disclose its subscribers' Private Viewing Information to Meta without asking for let alone obtaining its subscribers' consent to these practices.

5. The VPPA clearly prohibits what Defendant has done. Subsection (b)(1) of the VPPA provides that, absent the consumer's prior informed, written consent, any "video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person for," 18 U.S.C. § 2710(b)(1), inter alia, liquidated damages in the amount of $2,500.00 per violation and equitable relief, *see id.* § 2710(c).

6. Accordingly, on behalf of themselves and the putative Class members defined below, Plaintiff brings this Class Action Complaint against Defendant for intentionally and unlawfully disclosing his Personal Viewing Information to Meta.

PARTIES

I. Plaintiff Silva

7. Plaintiff Silva is, and at all times relevant hereto was, a citizen and resident of Bedford County in Alum Bank, Pennsylvania.

8. Plaintiff Silva is, and at all times relevant hereto was, a user of Meta.

9. Plaintiff Silva is a consumer of the video products and services offered on Defendant's masterclass.com website. He first subscribed to Defendant's website in or about December 2023 and has continuously maintained his subscription since then. Plaintiff Silva became a subscriber to Defendant's website by registering and paying for a subscription via the Google quick sign-up feature, which automatically pulled over his

name, email address, payment information, and zip code from his Google account.

10. On multiple occasions during the two years preceding the filing of this action, Plaintiff Silva used his subscription on Defendant's website to request and obtain pre-recorded videos from Defendant. On each such occasion, Defendant disclosed to Meta Plaintiff Silva's FID coupled with the specific title of the video he requested and obtained and the URL where he requested access to and obtained the video, among other information concerning Plaintiff Silva and the device on which he used to request and obtain the video.

11. At all times relevant hereto, including when purchasing a subscription to Defendant's website and accessing and obtaining the prerecorded video material provided to subscribers on Defendant's website, Plaintiff Silva had a Meta account, a Meta profile, and an FID associated with such profile.

12. Plaintiff Silva has never consented, agreed, authorized, or otherwise permitted Defendant to disclose his Personal Viewing Information to Meta. In fact, Defendant has never even provided Plaintiff Silva with written notice of its practices of disclosing its customers' Personal Viewing Information to third parties such as Meta.

13. Because Defendant disclosed Plaintiff Silva's Private Viewing Information (including his FID, the title of the prerecorded video materials he accessed and obtained from Defendant's website with his paid subscription, and the URL where such video is available to subscribers on Defendant's website) to Meta during the applicable statutory period, Defendant violated Plaintiff Silva's rights under the VPPA and invaded his statutorily conferred interest in keeping such information (which bears on his personal affairs and concerns) private.

II. Defendant Yanka Industries Inc. d/b/a MasterClass

14. Defendant is a Delaware Foreign Business Corporation with its headquarters and principal place of business located at 660 4th Street, San Francisco, CA 94107.

15. Defendant operates and maintains the website masterclass.com, where it sells subscriptions to consumers and provides its subscribers access to a digital library comprised of various types of pre-recorded instructional and educational videos.

JURISDICTION AND VENUE

16. This Court has subject-matter jurisdiction over this civil action pursuant to 28 U.S.C. § 1331 and 18 U.S.C. § 2710.

17. Personal jurisdiction and venue are proper because Defendant maintains its headquarters and principal place of business in San Francisco, CA, within this judicial District.

VIDEO PRIVACY PROTECTION ACT

18. Generally speaking, the VPPA prohibits companies like Defendant from knowingly disclosing to third parties like Facebook information that personally identifies consumers like Plaintiff as having viewed particular videos or other audio-visual products or services.

19. Specifically, subject to certain exceptions that do not apply here, the VPPA prohibits "a video tape service provider" from "knowingly disclos[ing], to any person, personally identifiable information concerning any consumer of such provider[.]" 18 U.S.C. § 2710(b)(1). The statute defines a "video tape service provider" as "any person, engaged in the business…of rental, sale, or delivery of prerecorded video cassette tapes

or similar audio visual materials," 18 U.S.C. § 2710(a)(4), and defines a "consumer" as "a renter, purchaser, or subscriber of goods or services from a video tape service provider." 18 U.S.C. § 2710(a)(1). "'[P]ersonally identifiable information' includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." 18 U.S.C. § 2710(a)(3)

20. The VPPA's purpose is as apropos today as it was at the time of its enactment over 35 years ago. Leading up to the statute's enactment in 1988, members of the United States Senate warned that "[e]very day Americans are forced to provide to businesses and others personal information without having any control over where that information goes." *Id.* Senators at the time were particularly troubled by disclosures of records that reveal consumers' purchases and rentals of videos and other audiovisual materials, because such records offer "a window into our loves, likes, and dislikes," such that "the trail of information generated by every transaction that is now recorded and stored in sophisticated record-keeping systems is a new, more subtle and pervasive form of surveillance." S. Rep. No. 100-599 at 7-8 (1988) (statements of Sens. Simon and Leahy, respectively).

21. Thus, in proposing the Video and Library Privacy Protection Act (which later became the VPPA), Senator Patrick J. Leahy (the senior Senator from Vermont from 1975 to 2023) sought to codify, as a matter of law, that "our right to privacy protects the choice of movies that we watch with our family in our own homes." 134 Cong. Rec. S5399 (May 10, 1988). As Senator Leahy explained at the time, it is the personal nature of such information, and the need to protect it from disclosure, that is the raison d'être of the statute: "These activities are at the core of any definition of personhood. They

reveal our likes and dislikes, our interests and our whims. They say a great deal about our dreams and ambitions, our fears and our hopes. They reflect our individuality, and they describe us as people." *Id.*

22. While these statements rang true in 1988 when the act was passed, the importance of legislation like the VPPA in the modern era of data mining is more pronounced than ever before. During a recent Senate Judiciary Committee meeting, "The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century," Senator Leahy emphasized the point by stating: "While it is true that technology has changed over the years, we must stay faithful to our fundamental right to privacy and freedom. Today, social networking, video streaming, the 'cloud,' mobile apps and other new technologies have revolutionized the availability of Americans' information."[1]

23. Former Senator Al Franken may have said it best: "If someone wants to share what they watch, I want them to be able to do so . . . But I want to make sure that consumers have the right to easily control who finds out what they watch—and who doesn't. The Video Privacy Protection Act guarantees them that right."[2]

24. In this case, however, Defendant deprived Plaintiff and the unnamed Class members of that right by systematically (and surreptitiously) disclosing their Personal

[1] The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century, Senate Judiciary Committee Subcommittee on Privacy, Technology and the Law, http://www.judiciary.senate.gov/meetings/the-video-privacy-protection-act-protecting-viewer-privacy-in-the-21stcentury.

[2] Chairman Franken Holds Hearing on Updated Video Privacy Law for 21st Century, frank.senate.gov (Jan. 31, 2012).

Viewing Information to Facebook, without providing notice to (let alone obtaining consent from) any of them, as explained in detail below.

BACKGROUND FACTS

I. Consumers' Personal Information Has Real Market Value

25. In 2001, Federal Trade Commission ("FTC") Commissioner Orson Swindle remarked that "the digital revolution . . . has given an enormous capacity to the acts of collecting and transmitting and flowing of information, unlike anything we've ever seen in our lifetimes . . . [and] individuals are concerned about being defined by the existing data on themselves."[3]

26. More than a decade later, Commissioner Swindle's comments ring truer than ever, as consumer data feeds an information marketplace that supports a $26 billion dollar per year online advertising industry in the United States.[4]

27. The FTC has also recognized that consumer data possesses inherent monetary value within the new information marketplace and publicly stated that:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[5]

---

[3] FCC, *The Information Marketplace* (Mar. 13, 2001), at 8-11, *available at* https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.

[4] *See Web's Hot New Commodity: Privacy*, Wall Street Journal (Feb. 28, 2011), http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html.

[5] Statement of FTC Cmr. Harbour (Dec. 7, 2009), at 2, *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

28. In fact, an entire industry exists while companies known as data aggregators purchase, trade, and collect massive databases of information about consumers. Data aggregators then profit by selling this "extraordinarily intrusive" information in an open and largely unregulated market.[6]

29. The scope of data aggregators' knowledge about consumers is immense: "If you are an American adult, the odds are that [they] know[] things like your age, race, sex, weight, height, marital status, education level, politics, buying habits, household health worries, vacation dreams—and on and on."[7]

30. Further, "[a]s use of the Internet has grown, the data broker industry has already evolved to take advantage of the increasingly specific pieces of information about consumers that are now available."[8]

31. Recognizing the serious threat the data mining industry poses to consumers' privacy, on July 25, 2012, the co-Chairmen of the Congressional Bi-Partisan Privacy Caucus sent a letter to nine major data brokerage companies seeking information on how those companies collect, store, and sell their massive collections of consumer data, stating in pertinent part:

---

[6] *See* M. White, *Big Data Knows What You're Doing Right Now*, TIME.com (July 31, 2012), http://moneyland.time.com/2012/07/31/big-data-knows-what-youre-doing-right-now/.

[7] N. Singer, *You for Sale: Mapping, and Sharing, the Consumer Genome*, N.Y. Times (June 16, 2012), *available at* http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of- consumer-database-marketing.html.

[8] Letter from Sen. J. Rockefeller IV, Sen. Cmtee. on Commerce, Science, and Transportation, to S. Howe, Chief Executive Officer, Acxiom (Oct. 9, 2012) *available at* http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=3bb94703-5ac8-4157-a97b-a658c3c3061c.

> By combining data from numerous offline and online sources, data brokers have developed hidden dossiers on every U.S. consumer. This large[-]scale aggregation of the personal information of hundreds of millions of American citizens raises a number of serious privacy concerns.[9]

32. Data aggregation is especially troublesome when consumer information is sold to direct-mail

33. Disclosures like Defendant's are particularly dangerous to the elderly. "Older Americans are perfect telemarketing customers, analysts say, because they are often at home, rely on delivery services, and are lonely for the companionship that telephone callers provide."[10] The FTC notes that "[t]she elderly often are the deliberate targets of fraudulent telemarketers who take advantage of the fact that many older people have cash reserves or other assets to spend on seemingly attractive offers."[11]

34. Indeed, an entire black market exists while the personal information of vulnerable elderly Americans is exchanged. Thus, information disclosures like Defendant's are particularly troublesome because of their cascading nature: "Once marked as receptive to [a specific] type of spam, a consumer is often bombarded with similar fraudulent offers from a host of scam artists."[12]

---

[9] *See Bipartisan Group of Lawmakers Query Data Brokers About Practices Involving Consumers' Personal Information*, Website of Sen. Markey (July 24, 2012), http://www.markey.senate.gov/news/press-releases/bipartisan-group-of-lawmakers-query-data-brokers-about-practices-involving-consumers-personal-information.

[10] *Id.*

[11] *Fraud Against Seniors: Hearing before the Senate Special Committee on Aging* (August 10, 2000) (prepared statement of the FTC), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-fraud-against-seniors/agingtestimony.pdf.

[12] *Id.*

35. Defendant is not alone in violating its customers' statutory rights and jeopardizing their well-being in exchange for increased revenue: disclosing customer and subscriber information to data aggregators, data appenders, data cooperatives, direct marketers, and other third parties has become a widespread practice. Unfortunately for consumers, however, this growth has come at the expense of their most basic privacy rights.

II. Consumers Place Monetary Value on their Privacy and Consider Privacy Practices When Making Purchases

36. As the data aggregation industry has grown, so too have consumer concerns regarding their personal information.

37. A recent survey conducted by Harris Interactive on behalf of TRUSTe, Inc. showed that 89 percent of consumers polled avoid doing business with companies who they believe do not protect their privacy online.[13] As a result, 81 percent of smartphone users polled said that they avoid using smartphone apps that they don't believe protect their privacy online.[14]

38. Thus, as consumer privacy concerns grow, consumers are increasingly incorporating privacy concerns and values into their purchasing decisions and companies viewed as having weaker privacy protections are forced to offer greater value elsewhere (through better quality and/or lower prices) than their privacy- protective competitors.

---

[13] *See 2014 TRUSTe US Consumer Confidence Privacy Report*, TRUSTe, http://www.theagitator.net/wp-content/uploads/012714_ConsumerConfidenceReport_US1.pdf.

[14] *Id.*

39. In fact, consumers' personal information has become such a valuable commodity that companies are beginning to offer individuals the opportunity to sell their personal information themselves.[15]

40. These companies' business models capitalize on a fundamental tenet underlying the personal information marketplace: consumers recognize the economic value of their private data. Research shows that consumers are willing to pay a premium to purchase services from companies that adhere to more stringent policies of protecting their personal data.[16]

41. Thus, in today's digital economy, individuals and businesses alike place a real, quantifiable value on consumer data and corresponding privacy rights.[17] As such, where a business offers customers a service that includes statutorily guaranteed privacy protections, yet fails to honor these guarantees, the customer receives a service of less value than the service paid for.

III. Defendant Systematically Discloses its Subscribers' Personal Viewing Information to Meta

[15] *See* Joshua Brustein, *Start-Ups Seek to Help Users Put a Price on Their Personal Data*, N.Y. Times (Feb. 12, 2012), *available at* http://www.nytimes.com/2012/02/13/technology/start-ups-aim-to-help-users-put-a-price-on-their-personal-data.html.

[16] *See* Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy Information on Purchasing Behavior*, 22(2) Information Systems Research 254, 254 (2011); *see also* European Network and Information Security Agency, *Study on monetising privacy* (Feb. 27, 2012), *available at* https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/monetising-privacy.

[17] *See* Hann, et al., *The Value of Online Information Privacy: An Empirical Investigation* (Oct. 2003) at 2, *available at* http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.321.6125&rep=rep1&type=pdf ("It is obvious that people value online privacy.").

42. As alleged below, when a subscriber to Defendant's website requests or obtains a specific video, the Meta Pixel technology that Defendant intentionally installed on its website transmits the subscriber's personally identifying information and detailed information concerning the specific interactions the subscriber takes on its website (including the subscriber's Private Viewing Information revealing the specific videos that he or she requested) to Meta, without the subscriber's consent and in clear violation of the VPPA.

A. The Meta Pixel

43. On February 4, 2004, Mark Zuckerberg and others launched Facebook, now known as "Meta".[18] Since then, Meta has become the world's largest social media platform. To create a Meta account, a person must provide, *inter alia*, his or her first and last name, birthdate, gender, and phone number or email.

44. The Meta Pixel, first introduced in 2013 as the "Facebook Pixel," is a unique string of code that companies can embed on their websites to allow them to track consumers' actions and report the actions back to Meta.

45. The Meta Pixel allows online-based companies like Defendant to build detailed profiles about their visitors by collecting information about how they interact with their websites, and to then use the collected information to service highly targeted advertising to them.

46. Additionally, a Meta Pixel installed on a company's website allows Meta "to match . . . website visitors to their respective [Meta] User accounts."[19] Meta is able

[18] Company Info, FACEBOOK, https://about.fb.com/company-info./.

[19] https://developers.facebook.com/docs/meta-pixel/get-started.

to do this because it has assigned to each of its users an "FID" number – a unique and persistent identifier that allows anyone to look up the user's unique Meta profile and thus identify the user by name[20] – and because each transmission of information made from a company's website to Meta via the Meta Pixel is accompanied by, *inter alia*, the FID of the website's visitor. Moreover, the Meta Pixel can follow a consumer to different websites and across the Internet even after clearing browser history.

47. Meta has used the Meta Pixel to amass a vast digital database of dossiers comprised of highly detailed personally identifying information about each of its billions of users worldwide, including information about all of its users' interactions with any of the millions of websites across the Internet on which the Meta Pixel is installed. Meta then monetizes this Orwellian database by selling advertisers the ability to serve highly targeted advertisements to the persons whose personal information is contained within it.

48. Simply put: if a company chooses to install the Meta Pixel on its website, both the company who installed it and Meta (the recipient of the information it transmits) are then able to "track[] the people and type of actions they take"[21] on the company's website, including the purchases they made, the items they spent time viewing, and, as relevant here, the specific video content that they requested or obtained

---

[20] For example, Mark Zuckerberg's FID is reportedly the number "4," so logging into Facebook and typing www.facebook.com/4 in the web browser retrieves Mark Zuckerberg's Facebook page: www.facebook.com/zuck, and all of the additional personally identifiable information contained therein.

[21] https://www.facebook.com/business/goals/retargeting.

on the website.

B. Defendant Knowingly Uses the Meta Pixel to Transmit the Private Viewing Information of all of its Subscribers to Meta

49. Defendant allow persons to become digital consumers of its various online-based video products and services by subscribing to its website. To subscribe, the consumer must provide at least his or her name, email address, billing address, and credit- or debit-card (or other form of payment) information.

50. After a person has completed the subscription process and gains access to videos on Defendant's website, Defendant uses – and has used at all times relevant hereto – the Meta Pixel to disclose to Meta the unencrypted FID of the subscriber and the specific videos that he or she requested or obtained from Defendant's website.

51. Defendant intentionally programmed its website (by following step-by-step instructions from Meta's website) to include a Meta Pixel that systematically transmits to Meta the FIDs of its subscribers and the video products that each of them requested in order to take advantage of the targeted advertising and other informational and analytical services offered by Meta.

52. With only a person's FID and the video content name or URL that the person requested on Defendant's website—all of which Defendant knowingly provides to Meta —any ordinary person could learn the identity of the person to whom the FID corresponds and the specific video products or services that this person requested. This can be accomplished simply by accessing the URL www.facebook.com/[unencrypted FID]/.

53. Defendant's practices of disclosing the Private Viewing Information of its

subscribers to Meta continued unabated for the full duration of the time period relevant to this action. At all times relevant hereto, whenever Plaintiff or another subscriber of Defendant's website requested a particular video (by clicking on it) on Defendant's website, Defendant disclosed to Meta that (*inter alia*) the specific video that was requested (including the URL where such video was accessed), along with the FID of the subscriber who requested it (which, as discussed above, uniquely identifies the person).

54. At all relevant times, Defendant knew that the Meta Pixel disclosed its subscribers Private Viewing Information to Meta.

55. Defendant could easily have programmed its website so that none of its subscribers' detailed Private Viewing Information is disclosed to Meta. Instead, Defendant chose to program its website so that all of its subscribers' detailed Private Viewing Information is sent to Meta *en masse*.

56. Prior to transmitting its subscribers' Private Viewing Information to Meta, Defendant failed to notify Plaintiff or any of its other subscribers that it would do so, and neither Plaintiff nor any of its other subscribers have consented (in writing or otherwise) to these practices.

57. By intentionally disclosing to Meta Plaintiff's and its other subscribers' FIDs together with the specific video content they each requested or obtained, without Plaintiff's or any of its other subscribers' consent to these practices, Defendant knowingly and systematically violated the VPPA on an enormous scale.

CLASS ACTION ALLEGATIONS

58. Plaintiff seeks to represent a class defined as all persons in the United

States who, during the two years preceding the filing of this action, requested or obtained video content from Defendant's website as a subscriber of Defendant's website and while maintaining an account with Meta Platforms, Inc. f/k/a Facebook, Inc.

59. Class members are so numerous that their individual joinder herein is impracticable. On information and belief, members of the Class number in at least the tens of thousands. The precise number of Class members and their identities are unknown to Plaintiff at this time but may be determined through discovery. Class members may be notified of the pendency of this action by mail and/or publication through the membership records of Defendant.

60. Common questions of law and fact exist for all Class members and predominate over questions affecting only individual class members. Common legal and factual questions include, but are not limited to: (a) whether Defendant knowingly disclosed Plaintiff's and Class members' Private Viewing Information to Meta; (b) whether Defendant's conduct violates the Video Privacy Protection Act, 18 U.S.C. § 2710; (c) whether Defendant should be enjoined from disclosing Plaintiff's and Class members' Private Viewing Information to Meta; and (d) whether Plaintiff and Class members are entitled to statutory damages for the aforementioned violations.

61. The named Plaintiff's claims are typical of the claims of the Class in that the named Plaintiff and the Class members suffered invasions of their statutorily protected right to privacy (as afforded by the VPPA), as well as intrusions upon their private affairs and concerns that would be highly offensive to a reasonable person, as a result of Defendant's uniform and wrongful conduct in intentionally disclosing their Private Purchase Information to Meta.

62. Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the Class members he seeks to represent, he has retained competent counsel experienced in prosecuting class actions, and he intends to prosecute this action vigorously. Plaintiff and his counsel will fairly and adequately protect the interests of Class members.

63. The class mechanism is superior to other available means for the fair and efficient adjudication of Class members' claims. Each individual Class Member may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by this case's complex legal and factual issues. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues.

CAUSE OF ACTION
Violation of the Video Privacy Protection Act, 18 U.S.C. § 2710

64. Plaintiff repeats the allegations asserted in the preceding paragraphs as if fully set forth herein.

65. Plaintiff brings his claim individually and on behalf of the putative Class Members against Defendant.

66. The VPPA prohibits a "video tape service provider" from knowingly disclosing "personally identifying information" concerning any "consumer" to a third party without the "informed, written consent (including through an electronic means using the Internet) of the consumer." 18 U.S.C. § 2710.

67. As defined in 18 U.S.C. § 2710(a)(4), a "video tape service provider" is "any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audiovisual materials[.]" Defendant is a "video tape service provider" as defined in 18 U.S.C. § 2710(a)(4) because it is engaged in the business of delivering audiovisual materials that are similar to prerecorded video cassette tapes and those sales affect interstate or foreign commerce.

68. As defined in 18 U.S.C. § 2710(a)(1), a "'consumer' means any renter, purchaser, or consumer of goods or services from a video tape service provider." As alleged above, Plaintiff and Class members, as paid subscribers to Defendant's website, are consumers of Defendant's service of providing video content. Thus, Plaintiff and Class members are "consumers" as defined in 18 U.S.C. § 2710(a)(1).

69. As defined in 18 U.S.C. § 2710(a)(3), "'personally identifiable information' includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." Defendant knowingly disclosed Plaintiff's and Class members' Private Viewing Information to Meta in the manner alleged herein. The Private Viewing Information that Defendant transmitted to Meta constitutes "personally identifiable information" as defined in 18 U.S.C. § 2710(a)(3) because the transmitted information identified Plaintiff and each Class member to Meta as an individual who requested or obtained video content, including

the specific video materials requested or obtained from Defendant's website.

70. Defendant never obtained informed, written consent from Plaintiff or any Class member to disclose their Private Viewing Information to Meta or any other third party. More specifically, Defendant never obtained from Plaintiff or any Class member informed, written consent in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer; Defendant never obtained from Plaintiff or any Class member informed, written consent that, at the election of the consumer, was given at the time the disclosure is sought or was given in advance for a set period of time, not to exceed two years or until consent is withdrawn by the consumer, whichever is sooner; and Defendant never provided an opportunity, in a clear and conspicuous manner, for Plaintiff or any Class member to withdraw consent on a case-by-case basis or to withdraw consent from ongoing disclosures, at the consumer's election. *See* 18 U.S.C. § 2710(b)(2).

71. Defendant knowingly disclosed such information to Meta because Defendant intentionally installed and programmed the Meta Pixel code on its website, knowing that such code would transmit to Meta the video titles requested by its subscribers and its subscribers' unique identifiers (including FIDs) when subscribers' requested or obtained videos from its website.

72. By disclosing Plaintiff's and Class members' Private Viewing Information, Defendant violated their statutorily protected right to privacy in the videos they requested or obtained from Defendant. 18 U.S.C. § 2710(c).

73. As a result of these violations, Defendant is liable to Plaintiff and Class members for damages and other relief as provided by the VPPA.

74. On behalf of himself and all members of the Class, Plaintiff seeks to enjoin Defendant's future disclosures of its subscribers' Private Viewing Information; liquidated damages in the amount of $2,500 per violation of the VPPA; reasonable attorneys' fees and costs; and all other preliminary or equitable relief the Court deems appropriate. 18 U.S.C. § 2710(c)(2)(A).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks a judgment against Defendant Yanka Industries Inc. d/b/a MasterClass. as follows:

A. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representatives of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

B. For an order declaring that Defendant's conduct as described herein violated the VPPA;

C. For an order finding in favor of Plaintiff and the Class and against Defendant on all counts asserted herein;

D. For an award of $2,500.00 to the Plaintiff and each Class member, as provided by the VPPA, 18 U.S.C. § 2710(c);

E. For an order permanently enjoining Defendant from disclosing the Private Viewing Information of its subscribers to third parties in violation of the VPPA.

F. For prejudgment interest on all amounts awarded; and

G. For an order awarding punitive damages, reasonable attorneys' fees, and costs to counsel for Plaintiff and the Class under Rule 23 and 18 U.S.C. § 2710(c).

JURY DEMAND

Plaintiff demands a trial by jury on all causes of action and issues so triable.

Dated: August 16, 2024

Respectfully submitted,

/s/ Frank S. Hedin

HEDIN LLP
FRANK S. HEDIN
535 Mission Street, 14th Floor
San Francisco, CA 94105
TELEPHONE: (305) 357-2107
FACSIMILE: (305) 200-8801
FHEDIN@HEDINLLP.COM

Counsel for Plaintiff and Putative Class